UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,791	04/02/2004	Marco Macchetti	02AG50553433	9927

27975 7590 11/01/2007

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
11/01/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

	Application No.	Applicant(s)	
Office Action Summary	10/816,791	MACCHETTI ET AL.	
	Examiner	Art Unit	
	Martin Jeriko P. San Juan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *April 2, 2004*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Remarks filed on September 18, 2007.

Claims 1-11 were originally cancelled. Claims 12-34 were originally pending.

Applicant has amended claims 17 and 28.

Claims 12-34 are currently pending.

The enclosed translation of PCT application no WO 03/010919 has been accepted and the cited reference has been considered.

Response to Arguments

1. Applicant's arguments filed on September 18, 2007 have been fully considered but they are not persuasive.

Applicant alleges that Coppersmith et al. fails to teach or suggest decoding the input byte and generating at least one bit string that contains only one active bit as in the claimed invention. Instead, the value retrieved from the s-box is substituted for the ith byte of original data from the current block resulting in a mixed byte, as highlighted in the above quote from Coppersmith et al. When the byte counter i is an even number s-box zero is used, and when i is an odd number s-box zero is used. The equation referenced by the Examiner in column 8, line 16, where C is defined, is used to generate a mixed byte that includes more than one active bit.

Examiner respectfully disagrees. The examiner cited equations starting in Col 8, Ln 16 as evidence that generating at least one bit string that contains only one active bit is taught by Coppersmith. It is because of this algorithm that S-boxes depicted in Fig 6 will be used [Col 8, Ln 62 thru Col 9, Ln 10]. Based on the equation, a byte (the input byte) coming from the block of data is used in the one-to-one binary function (as depicted in Col 8, Ln 16) to obtain the index of the substitution value. The substituted values are the output bytes of the generated data blocks of "mixed" bytes. Obtaining a substitution value will inherently involve decoding the index, which is a byte in length in the described embodiment, into a 256-bit string (signal) that will contain only one active bit because of the one-to-one property of the binary function. In other words, the index will only correspond or map to only one of the 256 entries contained in the S-box being used.

The Examiner is maintaining the rejections made in the previous action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claim 12, 14, 17, 20-21, 23-24, 26-28 and 33-34 is rejected under 35 U.S.C. 102(b) as being anticipated by Coppersmith et al. [US PN 6243470 B1].

a. Based on independent claim 12, Coppersmith et al. teach a method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function, the method comprising [This teaches the method of ciphering blocks of data in n-bit block segments.]: decoding an input byte [Col 7, Ln 57-60] and generating at least one bit string that contains only one active bit [Col 8, Ln 15, and Col 9, Ln 45. Cache access always involve some method of decoding the address into a n-bit string with an active bit used as a signal to select a single value at an addressed location; thus generating such string is inherent.]; logically combining bits of the at least one bit string according to the one-to-one binary function [Col 8, Ln 16. Obtaining a substitution value from an array is based on a one to one binary function.] and generating a 256-bit string [Col 9, Ln 22, The S-box array consist of 256 entries, and access to this array inherently expresses a 256-bit string whose active bit corresponds to an entry in the array.]; and encoding the 256-bit string for obtaining an output byte [The 256-bit string is encoded to correspond to the actual substitution byte to be obtained.].

b. With regard to dependent claim 14, Coppersmith et al. teach a method according to claim 12, wherein the input byte is decoded in a corresponding auxiliary 256-bit string; and the 256-bit string is obtained by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function [Col 8, Ln 15, and Col 9, Ln 45. The indexing value to be used for the s-box byte substitution undergoes a logical operation which inherently changes the order of the 256-bit string based on a 1-byte index.].

c. Claims 17, 23, and 28 are rejected using the same references as claim 12.

i. Claim 17 is still the same method that uses the same steps as claim 12.

ii. Claim 23 and 28 are both apparatus that performs the same method of claim 12.

d. Claims 20, 24, are rejected using the same references as claim 13.

iii. Claim 20 is still the same method that uses the same steps as claim 13.

iv. Claims 24 is the apparatus performing the method of claim 13.

e. Claims 26, 33, are rejected using the same references as claim 24.

v. Claims 26 and 33 are both apparatus having limitations that are inherent in references anticipating claim 24.

f. Claims 21, 27, and 34 are rejected using the same references as claim 14.

vi. Claims 21 is still the same method that uses the same steps as claim 14.

vii. Claims 27 and 34 are both apparatus that performs the same method of claim 14.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. Claim 13, 16, 22, 25, and 31-32 rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. [US PN 6243470 B1], and further in view of Ciraula et al. [US PN 5710731].

a. With regard to claim 13, Coppersmith et al. teach a method according to claim 12, but Coppersmith et al. do not teach the decoding that comprises subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the 256-bit string. Ciraula et al. teach a combined adder and decoder digital circuit that can decode an input byte by subdividing the input byte into a left nibble and a right nibble [Col 2, Ln 4-12. Ciraula et al. teach a tree based decoding scheme that subdivide the initial N-bit input into groups, thereby, teaching the subdividing of an input byte into two groups of half-bytes or nibbles.]. Each group generates a 16-bit string containing only one active bit, and wherein logically combining the bits comprises logically combining the 16-bit strings for generating the 256-bit string [Col 2, Ln 4-12]. It would have been obvious to one of ordinary skill in the art at the time of the invention to use the combined adder and decoder digital circuit into the method of Coppersmith et al. because such a digital circuit is necessary in the method of Coppersmith et al. that involves byte access in memory or on-chip cache especially for the one-to-one binary function [US 5710731, Col 1, Ln 13-25]. The suggestion/motivation for combining would have been to improve microprocessor (or cryptographic processor) performance [US 5710731, Col 1, Ln 38-42]. Therefore, it would have been obvious to combine Coppersmith et al. and Ciraula et al. to obtain the invention as specified in claim 13.

b. Claim 16 is rejected using the same references and rationale as claim 13 because Ciraula et al. teach the same combined adder and decoder digital circuit, wherein each bit of the output string is obtained by ANDing among the bits of the subdivided input strings [US 5710731, Col 2, Ln 9-12.].

c. Claim 31 is rejected using the same references and rationale as claim 13.

i. Claim 31 is the apparatus performing the same method of claim 13.

d. Claims 22, 25, and 32 are rejected using the same references and rationale as claim 16.

ii. Claim 22 is still the same method performing the method claim 16.

iii. Claim 25 and 32 are both apparatus that performing the method of claim 16.

2. Claims 15, 18-19, and 29-30 rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. [US PN 6243470 B1], and further in view of Morioka et al. [IDS Morioka et al, 2002].

a. With regard to claim 15, Coppersmith et al. teach the method according to claim 12, but Coppersmith et al. do not teach wherein the one-to-one binary function represents a ByteSub operation of a Rijndael AES encryption/decryption algorithm. Morioka et al. teaches optimizing S-box circuits that represent the ByteSub operation of the Rijndael AES encryption/decryption algorithm.
It would have been obvious to one of ordinary skill in the art at the time of the invention to use the method of Coppersmith et al. to represent the ByteSub operation as the optimized S-box circuit of the Rijndael AES encryption/decryption algorithm as depicted by Morioka et al. because the method of Coppersmith et al. can be used as a sub-function of the Rijndael AES encryption/decryption algorithm. The suggestion/motivation for combining would have been to optimize the S-box circuit of the Rijndael AES design for low power consumption [Morioka et al., abstract]. Therefore, it would have been obvious to combine Coppersmith et al. and Morioka et al to obtain the invention as specified in claim 15.

b. Claims 18-19, and 29-30 are rejected using the same references and rationale as claim 15.

i. Claims 18-19 are still the same method performing the method of claim 15.

ii. Claims 29-30 are both apparatus performing the method of claim 15.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner. Art Unit 2132

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100